01 | 回顾前世：解读区块链技术发展三阶段

2021-07-21 赵铭

《说透区块链》 课程介绍 >

讲述：赵铭
时长 14:46 大小 13.53M

你好，我是赵铭。

区块链概念自出现到如今不过短短十几年，却深刻地影响着我们的工作跟生活。

在专栏的第一部分，我想先跟你讲讲区块链技术的发展历史及现状。任何一种技术，在发展过程中，往往会因为各种原因偏离创立者的初衷，区块链技术也一样。

回顾技术发展的历史，能够让我们理清前因后果，更深刻地认识这项技术是怎样演变成现在的样子；而了解技术发展的现状，又可以帮我们更好地看清技术发展脉络及未来方向。

而这一讲，我们重点关注区块链技术的发展历史。

萌芽期

相信说起金融危机，你我都会谈虎色变。最近的一次世界级金融危机就在 2008 年，这次危机让很多先行者对现代金融体系逐渐失望。在这样的时代背景下，比特币应运而生。

比特币的发明者中本聪敏锐地意识到，大部分的互联网贸易结算都依赖**可信任的第三方金融机构**处理，尽管在大多数时候这些系统的运转是足够好的。可是一旦遇上极端信任危机，信任关系的失衡就会导致现代金融体系的结构性塌陷。

常规的思路几乎失灵，但中本聪却另辟蹊径，提出了一种全新的解决方案，一个自由主义者拯救世界的故事就此拉开帷幕。这个方案最出彩的其实有两点，第一就是**还原了支付原来的样子**，第二就是**创新性地引入了支付脚本**，我分别给你说一说。

什么是支付本来的样子呢？你可以这样理解，贸易支付的本质其实是买家与卖家的供需关系，只是由于买卖双方的不信任，才需要引入双方都信任的第三方进行担保，为双方的买卖行为背书。在中本聪看来，这种由信任作为媒介的运行模式是有问题的。

所以，中本聪想到了去掉第三方担保的可能性，设计了一套基于密码学、无需买卖双方彼此信任就可以完成支付的数字货币系统。

在剔除信任纽带之外，比特币还创新性地引入支付脚本用于货币的支付。脚本实质是一段计算机程序代码，如果你可以输入正确的参数，脚本执行成功就意味着你拥有货币的使用权。所以我们可以认为，比特币通过程序脚本，实现了一个完全严格按照计算机逻辑运行的数字货币转移机制。

但是，比特币的脚本功能并不完美，它只支持指令的顺序执行。而一般功能完善的计算机编程语言都支持顺序、分支以及循环。诚然，只基于顺序执行的脚本可以实现比特币的条件支付，但也仅限如此。

这里可以假设你有一个这样的需求：

> 抵押自己的一套房产，换 10 枚比特币，并约定 1 年以后用 11 枚比特币解压房产；如果未能守约，房产将被法拍。

现在我们将这段描述转换成计算机语言，很容易就能发现，这段逻辑必须要有分支的判断，如果满足条件解压房产，不满足条件，房产将被拍卖。比特币可以实现这个需求吗？

很明显，因为比特币脚本没有分支判断能力，因此实现不了。而**现代社会是一个多元融合的世界，任何事物都不可能独立地存在，尤其是在金融支付领域**。比特币仅将自身定位为加密货币，在复杂的契约逻辑面前是无能为力的。

有人看到了这种局限，他就是以太坊的创始人，V 神。

诞生期

在研究比特币的过程中，V 神逐渐认识到，比特币背后的区块链技术不光可以用在加密货币中，还有更多可能性，但比特币的架构却阻碍了技术的发展，因此他希望能够扩展比特币的脚本功能，使其更加智能。

如果直接在比特币上打补丁，其扩展能力也极为有限。因此，V 神将他的精力集中到如何创建一个替代比特币的解决方案中，不久就发表了以太坊白皮书《以太坊：一个下一代加密货币和去中心化应用平台》。

在白皮书中，V 神阐述了以太坊构架愿景：在加密货币的基础上，增加智能合约功能，这样开发者就可通过智能合约编程把一切有价值的客观 / 主观事物锚定到以太坊进行交易，实现价值的传递。这也就是**区块链发展的最终形态是价值网络**这个论调的由来。

智能合约到底是怎样发挥作用的呢，我接着前面房屋产权登记的例子解释一下。有了相关部门的数字证明，业主就可以通过智能合约把房产证等信息转换成可交易的数字资产。当然这个过程是长期的，需要区块链在社会治理领域落地以后才可实施。

2015 年 7 月 30 日，以太坊主网正式启动，以太坊从此走上历史的舞台。

以太坊的核心我们可以认为就是智能合约的加持。而智能合约是软件工程师基于以太坊协议，自主编写的程序代码。不过我们都清楚，天底下几乎不存在没有 BUG 的软件系统，且以太坊智能合约是开源的，任何人都可以随时随地查看部署在以太坊上的智能合约源码，这就给黑客钻漏洞留下了空子。

最著名的一次黑客攻击事件发生在 16 年 4 月，黑客将The DAO合约中锁定的价值约 1.5 亿美元的以太币偷走约 6000 万美元，并立刻在交易所抛售，给整个加密货币市场造成了不可挽回的损失。

黑客事件发生以后，以太坊社区发生了激烈的讨论。一部分人主张将以太坊主网回滚至黑客攻击之前；而另一部分人崇尚无为而治，主张不应该依靠外力干预已被认可的既定事实。可以说这是对区块链信仰的一次重大考验。

然而，经过社区讨论，16 年 7 月 20 日进行以太坊硬分叉，将以太坊主网分裂成两个网络，ETH 以及 ETC。ETH 删除了黑客攻击的一切痕迹，并将被盗走的以太币归还给原始拥有者，现在我们所说的以太坊指的就是**回滚**的这一分支。而 ETC 则保留了黑客攻击在内的全部交易，以保持区块链赖以生存的去中心化以及不可篡改的基本原则。

正是因为这一事件，直接导致了后续区块链的野蛮生长。

野蛮生长期

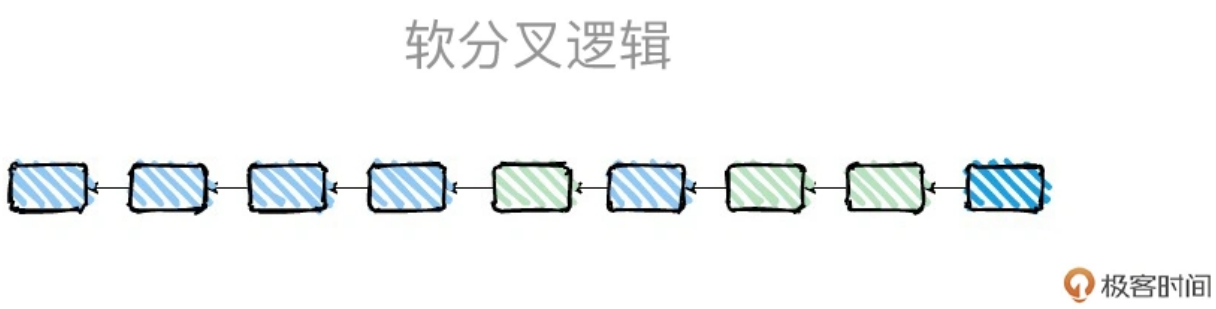
软分叉和硬分叉

为什么 The DAO 事件会直接推动后续区块链的野蛮发展呢？且听我慢慢为你道来。

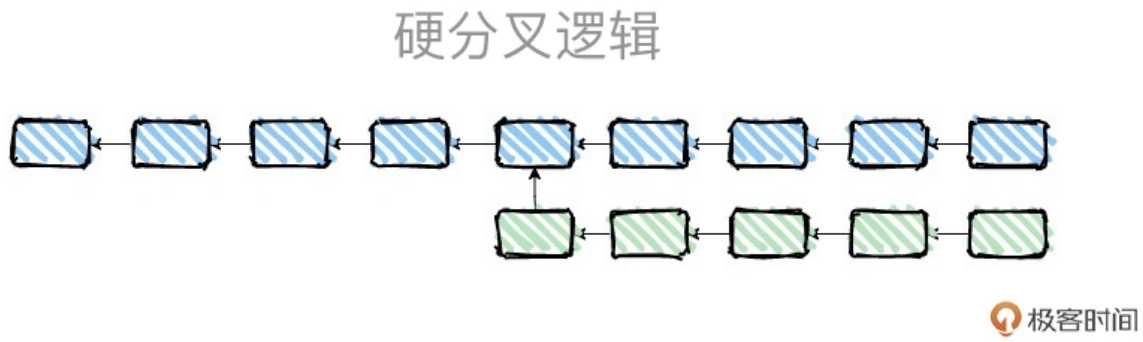
所有的软件系统都会有 BUG。一般情况下，我们会在之前软件版本的基础上修改源码，新版本相比旧版本只有部分逻辑的不同，程序基本规则也没有太大的变化，两个版本的程序之间简单做些适配，就可以互相认知，可以说是无缝兼容的。我们把这种情况称之为迭代。

而另一些时候，因为架构的调整、规则的变更，两个版本的程序之间已经无法兼容。这时我们就无法称之为迭代了，而是用重构指代这种变化。通常情况下，多次迭代叠加的结果就是重构，可以理解为量变引起质变。

而在区块链中，网络是由多个节点彼此相连组成的，节点间必须可以互相通信。几个小版本的软件迭代不影响区块链网络的运行，一些节点升级，而另一些节点继续使用原始版本，是不会引起区块链网络的割裂。**这种情况就是所谓的软分叉，其本质就是可兼容的程序版本更新。**



而一旦社区决定对区块链协议进行了重构，则必须协调整个网络节点都进行升级。你可以设想一下，如果一半节点继续使用原来的版本，而另一部分节点升级了新版本的程序，在这种情况下，一个区块链网络就被割裂成了两个。虽然他们的数据从属于共同的祖先，但是在某一时刻，他们独自派生出不同的数据走向。**这就是硬分叉的逻辑，其本质是不可兼容的程序版本更新。**



这就不难解释，为什么每一次区块链网络的升级都是一件大事，需要社区去协调从哪一个区块启用新版本，废弃老版本。

回到 The DAO 事件本身，以太坊通过硬分叉分裂成 ETH 跟 ETC，两个网络都保持独立运营。从逻辑上讲，并没有什么问题，是可以说得通的。

但坏就坏在其凭证是有价值的，在硬分叉前，我拥有 1 枚 ETH，而硬分叉以后，我既有 1 枚 ETH，同时我又拥有了 1 枚 ETC。相当于我在什么都没有操作的情况下，凭空多了一枚有价值的凭证，虽然其价值可能相较原始的 ETH 来说相对较低。

“潘多拉的盒子”被打开了。

一些人的心思被解放了。如果我有理由述说比特币 / 以太坊存在的不足，提出解决方案，写一个白皮书，阐述我的观点及实现路径。我是不是也可以通过硬分叉的方式，创造属于

我的区块链呢？

同时，如果我能拉人站台，让他们为我拉票，是不是也会有更多的人认同我的观点？通过这样的操作，是不是也逐渐有人会为我的理想买单，而一旦有人为我买单，我就凭空创造了“财富”泡沫。

一场轰轰烈烈的造链行动就开始了，各类基于硬分叉的旁系网络开枝散叶。最高兴也是最能推动这场行动的人，其实还并不是其创造者，而是在硬分叉前持有 BTC/ETH 的散户，他们得到了数不清的旁系凭证，当然希望其价值更高。所以他们就不断鼓动身边的人进场，进而不断推动这虚假的繁荣。

不可描述的推手

除硬分叉外，野蛮的背后还有不可描述的推手，因为某些众所周知的原因，不宜多说。

自有了这不可描述的推手之后，就像鱼遇到了水，一切都那么的自然。市场迎来了新一轮的疯狂。任何人只要有一些跟区块链沾点边的点子，都可以立马写一篇白皮书，找一群人运营社区，宣传自己的理想，换取投资人的赏识，蛊惑他们用真金白银为自己的“理想”买单。

不可否认，最初确实有很多团队真正在依靠这种融资的方式认认真真做事，但市场并不会因为你的认真给予你等比例的回报，反而是那些牛皮吹上天的赚到了大钱，且扰乱了市场。只有你想不到，没有他们做不到。

疯狂并没有持续太久，泡沫被无情刺穿。自此，市场逐渐冷清。时间就来到了区块链发展的新阶段，也就是现在，在下一讲中我将详细为你描述区块链技术的现状。

总结

在这一讲中，我阐述了我对区块链技术自萌芽到野蛮发展的三个历史阶段的认知。**比特币，以太坊是一种现象，而区块链技术是其背后的本质**。

区块链技术萌芽于比特币，诞生在以太坊，经历过乱象丛生的爆发，但也正是因为那些疯狂岁月，让千千万万个你我知道并了解到区块链技术。

历史无对错，只有结果。希望你通过我的讲解能够了解区块链技术的历史发展进程，并对区块链技术的未来充满想象及期待。

1.金融危机背景下，中本聪看到现代金融体系的不足，创建基于密码学而非信任关系的数字货币系统——比特币。

2. V 神在比特币的基础上，将智能合约与区块链结合，创立去中心化应用平台——以太坊。

3.The Dao 事件驱动历史进入野蛮生长期。

说透区块链

赵铭 | 区块链服务平台资深架构师

讨论

你是何时接触比特币，了解区块链技术的呢？在过去的十多年中，你有哪些与区块链的不解之缘？

扩展阅读

我非常建议你可以尝试阅读一下比特币白皮书以及以太坊白皮书，它们可以说是区块链领域的圣经。而且你也可以顺便了解一下中本聪及V 神这两个人，都是颇具传奇色彩的人物。

欢迎你在留言区跟我互动，主动思考、积极交流会让你更有收获。如果这节课对你有帮助，也欢迎你把这节课分享给自己的朋友、同事。

分享给需要的人，Ta订阅后你可得 20 元现金奖励

赞 1 提建议

© 版权归极客邦科技所有，未经许可不得传播售卖。 页面已增加防盗追踪，如有侵权极客邦将依法追究其法律责任。

上一篇 开篇词 | 区块链，一种面向未来的思维方式

精选留言 (1)

写留言

静静聆听

2021-07-21

币圈热消退，才慢慢让链圈的价值真正体现出来，区块链越是了解，越是觉得牛掰

作者回复: 静静聆听，你好。是这样的，没有币圈曾经的狂热，不会有区块链今天的发展；当然，如果没有国家政策的倾向，情况也会有所不同。二者算是相辅相成，共同推动区块链技术继续向前。